Anno 3 – N. 63
18 Novembre - 2 Dicembre 2004

**hack·er (hăk'ər)**
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

**Boss:** TheGuilty@hackerjournal.it

**I Ragazzi della redazione europea:**
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Simone Tarantino, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Silvio De Pecher, Contents by MDR

**Service:** Cometa s.a.s.

**DTP:** Davide "Fo" Colombo
Elenina "M&nosin@" Varesi

**Graphic designer:** Dopla Graphic S.r.l.
info@dopla.com

**Copertina:** Daniele Festa

**Publishing company:**
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

**Printing:**
Roto 3

**Distributore:**
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

**Distributore per l'estero:**
Johnsons International News Italia Spa
Via Valparaiso, 4
20144 Milano - Italia

**Abbonamenti:**
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15 - Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.



# editoriale

## L'hackumer **ha acume**

*Con tutte le parole che si inventano ogni giorno, ne inventiamo una anche qui: hackumer. L'hackumer è un hacker ma anche un consumer. Sì, un consumatore. Non c'è niente di male. Abbiamo tutti un computer, un provider, magari una stampante o un lettore MP3. Lo abbiamo comprato o qualcuno lo ha comprato per noi. Essere hacker non significa essere fuori dal mercato. Se mai, significa essere nel mercato più di chiunque altro, come vorrei spiegare entro poche righe.*

*Non è un caso che hackumer suoni tanto come la parola acume. Acutezza, ingegno vivo e pronto, recita il vocabolario. L'hacker può starsene nella sua stanzetta da solo a scoprire quanto è bravo. Può anche guardarsi allo specchio e farsi la congratulazioni. Ma serve a poco, se non diventa hackumer.*

*È l'hacker immerso nella vita di tutti i giorni che fa veramente la differenza. È attento ai monopoli e alle disonestà delle aziende. Vigila sulle libertà individuali e controlla che lo Stato faccia il suo mestiere (garantire le libertà) senza esagerare. Non ruba e rispetta i copyright, ma è il primo a ribellarsi appena la tutela dei diritti diventa abuso dei discografici, o dei politici, o dei terroristi, o di qualsiasi altro.*

*Se ci pensiamo è la stessa la differenza che c'è tra l'hacker secchione che tiene il suo sapere nascosto nel cassetto e e l'hacker vero, che diffonde il suo sapere e lo mette a disposizione di tutti. Se sei hacker hai desiderio per la conoscenza, e ne accumuli. Ma vuoi anche portarla a chiunque. Per farlo devi accettare il confronto, il dialogo, il disaccordo di qualcuno. In poche parole, l'hacker che fa il suo "lavoro" è dentro un mercato. Semplicemente è il mercato delle idee e delle opinioni.*

*Nel mercato delle idee stiamo facendo un ottimo lavoro. In quello dei beni bisogna fare di più. Il software è dominato da un monopolista. Le connessioni telefoniche sono dominate da un monopolista. La musica è dominata dalle case discografiche, che sono perfino peggio dei monopolisti. Si può andare avanti ancora molto.*

*Invece il tempo di parlare è finito. È tempo di cose concrete. Di farsi sentire, certo, ma darsi da fare. Mettere a disposizione le nostre capacità e le nostre idee per provocare cambiamenti concreti. Anche fare qualcosa di piccolo è estremamente importante. Forza. Hacker, sì. Ma servono pure gli hackumer.*

***theguilty@hackerjournal.it***

**HACKER JOURNAL: INTASATE LE NOSTRE CASELLE**

**Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!**

**redazione@hackerjournal.it**

# Ladri di ADSL

**Che serva o meno, facciamo sentire la nostra voce contro le tariffe insulse e ingiuste della banda larga in Italia!**

**L'iniziativa è nata sul forum del sito Hardware Upgrade,** alla pagina http://news.hwupgrade.it/13106.html. Si parlava di tariffe ed è emerso lo scandaloso divario che ci separa dalla Francia. L'esempio è appropriato perché non si parla di Paesi come l'Inghilterra o l'Irlanda, dove il mercato è di altro tipo e magari le tasse sono molto più basse delle nostre. La Francia è un Paese statalizzato forse ancora più dell'Italia, la pressione fiscale è assimilabile e anche lì ci sono forti monopoli, o ex monopolisti che fanno lo stesso il bello e il cattivo tempo come la nostra amata Telecom.

**Solo perché si chiama Alice non significa che viviamo nel paese delle meraviglie, Tutt'altro!**

**Ma non solo Telecom: pure altri provider internazionali, come Tiscali e Tele2,** giocano poco pulito, anche se in Italia hanno l'attenuante di fornire i loro servizi sopra linee Telecom e quindi i loro prezzi non possono allontanarsi troppo da quelli di Fernanda Lessa (testimonial di Alice, per capirci).

**Come si può vedere nella nostra tabellina, la situazione è veramente da rivoluzione.** La qualità del servizio, lo sappiamo tutti, è davvero bassa. Invece i prezzi sono pazzescamente alti, a volte anche più che doppi. In tasca di chi finiscono questi soldi? Lo Stato? Telecom? Qualche azionista? Sicuramente ben poco va a vantaggio del miglioramento dei servizi.

**Ecco la ragione per cui incoraggiamo a firmare la petizione online all'indirizzo** http://www.petitiononline.com/adsl04 it/petition.html. Non facciamoci illusioni: le petizioni online non hanno alcun valore giuridico e la nostra firma è poco più di un atto simbolico. Ma se passiamo da lì e lasciamo un clic, quantomeno se ne parla, prendiamo coscienza e alla fine può darsi che succeda qualcosa. Fosse anche passare a FastWeb, che ha prezzi ancora più alti, ma almeno fornisce vera banda larga in fibra ottica (dove arriva).

Barg the Gnoll
gnoll@hackerjournal.it

## Cara ADSL

**Se i cavi francesi arrivassero in Italia potremmo risparmiare cifre stratosferiche.** Si salva solo, un po', Tiscali...

| PROVIDER (SITO) | BANDA (KBPS) | PREZZO (euro/mese) |
|---|---|---|
| www.tele2.it (IT) | 640 | 33,95 |
| www.tele2.fr (FR) | 1024 | 14,85 |
| www.tele2.fr (FR) | 2048 | 19,85 |
| www.aliceadsl.it (IT) | 640 | 36,95 |
| www.aliceadsl.it (IT) | 1024 | 64,95 |
| www.aliceadsl.fr (FR) | 1024 | 5,48 |
| www.aliceadsl.fr (FR) | 3072 | 12,48 |
| abbonati.tiscali.it/adsl (IT) | 2048 | 29,95 (promozione) |
| abbonati.tiscali.it/adsl (IT) | 6144 | 69,95 (promozione) |
| abbonati.tiscali.it/adsl (IT) | 12288 | 99,95 (promozione) |
| register.tiscali.fr/adsl (FR) | 512 | 20 |
| register.tiscali.fr/adsl (FR) | 1024 | 30 |
| register.tiscali.fr/adsl (FR) | 2048 | 30 |

# ROBA DA SPIE IN ITALIANO

*Sul numero scorso abbiamo parlato di gaggeggi strani e affascinanti, da vere spie. Eccoli anche in Italia, importati e italianizzati da Giochi Preziosi. Sono le meraviglie di SpyGear (http://spygear.net).*
*Li troviamo nei negozi di giocattoli, naturalmente, ma anche perfino negli autogrill delle autostrade!*

# SUSE LINUX BECCATO

**Il kernel 2.6 della distribuzione Linux Suse** è gravemente bacato. Se si invia un pacchetto TCP opportunamente modificato, si può spegnere il sistema attaccato.
Le vulnerabilità sono presenti in Suse Linux 9.1 e Suse Linux Enterprise Server (SLES) 9; Suse Linux 9.2 non ha problemi perché contiene già il fix della versione di kernel 2.6.8.
Il livello di importanza che è stato assegnato a questo bug è 9/10, quindi una aggiornamento è vivamente consigliato a tutti quelli che stanno utilizzando il kernel bucato.
Il bollettino Suse che riguarda la vulnerabilità lo troviamo all'indirizzo http://www.suse.de/de/ security/2004_37_kernel.html, assieme alle istruzioni per scaricare la giusta patch.

## IL BUG HA GIÀ LA SUA PATCH

## SFILZA di PATCH per WINDOWS

*Non c'è super service packet 2 che tenga: si ricomincia con la collana di patch e questa volta dalle caratteristiche preoccupanti: su dieci rilasciate, sette sono classificate critiche e tre importanti. Sono etichettate da MS04-029 a MS04-038: tutte rilasciate nel corso del mese di ottobre.*

## » DISEGNA SU CELLULARE

**Philips 755**: si scatta, si aggiunge qualcosa di personale disegnandolo sul display e si invia. Un cellulare che aggiunge qualcosa alla marea di telefonini ormai tutti simili. Vale una news, almeno per l'idea.

## » NUOVO IPOD A COLORI E CON FOTO

**In 181 grammi**, il nuovo iPod Photo ci permette di andare in giro con 15.000 canzoni e 25 mila immagini da 4 megapixel, abbastanza per coprire una superficie di circa 450 mq! È disponibile in due modelli: con un disco da 40GB al prezzo di 559,00 euro e con 60GB 679,00 euro.

Certamente non poco, ma vogliamo mettere avere il display a 65 mila colori retroilluminato? Ovviamente da integrare con iTunes 4.7, il software che permette il trasferimento di tutti dati da e per iPod, disponibile sia per Mac che per Windows.

## » DIRITTI IN PIÙ PER IL P2P

**La frontiera della guerra tra P2P e industrie discografiche è in America**, e da là arriva una buona notizia: una corte della Pennsylvania ha stabilito che, quando le major discografiche chiedono di perseguire un presunto pirata musicale, quest'ultimo ha diritto

# HOT NEWS

## PER GENITORI PARANOICI

**Si applica allo zainetto di scuola dentro un apposito astuccio e contiene un sistema GPS e un allarme GSM.** È dotato di un pulsante antipanico che, se premuto, invia un segnale di allarme al genitore apprensivo, il quale può capire dalle coordinate il punto esatto della terra su cui ci troviamo. Nessuno scampo in caso di bigiate. Nemmeno se siamo andati solo un attimo in bagno... Tranquilli, per ora è pensato per i genitori giapponesi. I nostri non hanno ancora avuto la possibilità di vederlo.

## STAI DICENDO IL FALSO!

**Basta dire all'amico di appoggiare due dita sulle placche rosse del nostro nuovo orologio e fargli una domanda.**
La lunghezza di una barra sul display ci darà immediatamente l'idea se sta dicendo la verità oppure no. Ovvio che anche un'occhiatina alla faccia che farà potrà sempre aiutare la tecnologia di questo gadget. Tutte le info all'indirizzo: www.smarthome.com/9512.html

## VULNERABILITA' in REALPLAYER

**La colpa è però di Microsoft, che era già corsa** ai ripari pubblicando un bollettino e un aggiornamento Windows che troviamo qui: http://www.microsoft.com/technet/security/bulletin/ms04-034.mspx
Si tratta infatti di un file dunzip32.dll, la libreria di compressione utilizzata per creare file .zip con il comando Cartelle Compresse. La funzione è utilizzata da Real Player per aprire le skin, ma presenta un problema tale per cui è possibile fare girare sulla macchina ospite del codice autonomo.
La gravità del problema ha consigliato a Real Player di fornire comunque un proprio aggiornamento al suo lettore che così pone comunque fine a tutti i rischi.

## FOTOGRAFIE A 8 MEGAPIXEL

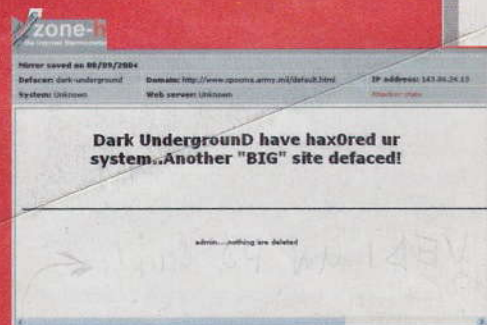
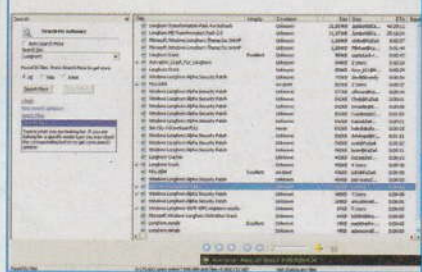
*Sharp ha annunciato un nuovo chip CCD a 8 megapixel che occupa lo stesso spazio di un normale CCD da 4 o 5, per cui può rimpiazzare quelli attualmente utilizzati sulla maggior parte delle macchine fotografiche digitali. La corsa alla massima risoluzione continua…*

di essere avvisato prima che il suo provider fornisca informazioni alle autorità. Il fatto è importante perché la RIAA, la potente organizzazione che raccoglie tutta l'industria musicale americana, ha intentato migliaia di cause contro ignoti, basandosi semplicemente sul loro indirizzo IP. Ora, se vengono rintracciati, gli ignoti avranno almeno diritto di sapere che sono indagati, prima di ritrovarsi la polizia che gli bussa a casa.

**Speriamo che difendano le loro navi meglio dei loro siti!**

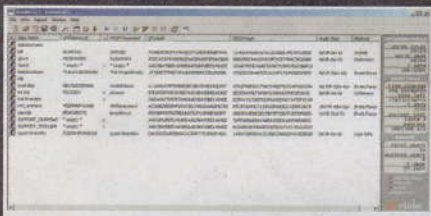
## UNDERGROUND ITALIANO DEFACCIA SITI MILITARI USA

**Il gruppo italiano conosciuto come dark underground** è riuscito a defacciare due importanti siti della marina militare americana e dell'esercito americano. Nel messaggio l'assicurazione che nessun contenuto è stato toccato, ma la sfida è riuscita e lo smacco per i webmaster dei siti militari è cocente. Tanto che uno di questi siti non era ancora stato rimesso in piedi una dozzina di giorni dopo l'incursione.

# MAIL TO: REDAZIONE@HACKER

## Quando commetti un reato

*Ciao, se uno commette un reato con Kazaa o altri programmi di p2p, viene avvisato via e-mail?*

*giorgia_palmas_ti_amo*

**Certamente no! Se vieni avvisato, è perché la Finanza sta bussando alla tua porta.**

## Una vecchia stupida password

*Ho un computer vecchiotto che mi sta dando problemi. Quale occasione migliore per passare a Linux? Solo che tutte le distribuzioni mi richiedono di aprire il BIOS e impostare il lettore CD come drive primario… e un paio di anni fa, quando ero ancora un ragazzotto e usavo il computer solo per far danni, ho messo la pass al BIOS… e non la ricordo più!*

*Alakan*

**Puoi ricorrere a programmi di craccatura delle password del BIOS come, per esempio, quelli elencati a http://www.password-crackers. com/crack.html.**

## Veloce come il menu Start

*Vorrei sapere come si imposta la velocità della barra avvio di windows 9x, ME e XP. Volevo sapere inoltre se c'è un comando DOS che, inserito in un file bat, permetta di creare file casuali.*

*DRHAckO*

**Non abbiamo capito che cosa intendi per file casuali, ma a http://david.tribble. com/dos/filldisk.bat trovi un file batch che riempie un disco con grossi file (occhio a usarlo sul disco di sistema...) e contiene comandi che dovrebbero esserti utili.**
**Altrimenti, http://www.chmaas.handshake.de/delphi/freeware/freeware.htm contiene i file RNDFILEC.EXE e RINDFILE.EXE che dovrebbero ugualmente fare al caso tuo.**

**Devi usare il Registro di configurazione, ovviamente. Lo lanci scegliendo Esegui dal menu Start e scrivendo regedit. Vai a HKEY_CURRENT_USER\Control Panel\desktop e aggiungi una voce MenuShowDelay, con un valore in millisecondi.**
**Il default è 400; numeri minori di 400 aumentano la velocità di risposta del menu. Con il programma TweakUI (http://www.annoyances.org/exec/show/gettingstarted) puoi fare la stessa cosa in modo grafico, utilizzando il comando Menu Speed. Scaricando http://rosecity-downloads. com/menushowdelay.reg e facendoci sopra un doppio clic si può impostare automaticamente la risposta a zero millisecondi.**

## Siti dei lettori

*Ciao! Sono domenico249 e vorrei segnalarvi il mio sito WML all'URL http://domenico249. altervista.org/index.wml.*

*domenico249*

*Volevo segnalare il sito della mia crew… http://www.hackerlaws.tk.*

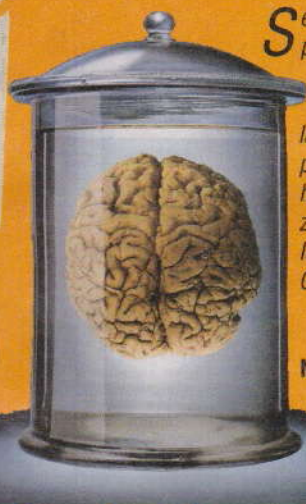
*Saluti, z3ro*

## Per fare un albero

*Come si fa a fare un virus?*

*huka*

**Si impara a programmare, possibilmente in assembler o comunque linguaggi di basso livello. Si impara il funzionamento interno dei sistemi operativi, quindi il funzionamento delle reti e dei protocolli di rete. In più si studia il funzionamento dei virus esistenti. Sui siti dei produttori di antivirus ci sono schede che sono ottimi punti di partenza.**
**Infine si impara che creare un virus può essere un buon esercizio di programmazione ma non è mai una cos intelligente se si ha intenzione di mandarlo in giro.**

# Se questo e' un hacker

*Secondo me hacker si nasce. Un hacker è una persona buonissima, che non ha bisogno di far vedere di essere un duro perché dentro ha la sicurezza del sapere, e non trova i difetti della vita per scopi di lucro o per divertimento, ma per aiutare gli altri ad eliminarli. Il cervello di un hacker è ipersviluppato. Fa parte di una generazione del futuro che eliminerà le forme di violenza e il male in generale. Sono veri e propri GENI...*

*Gh14Cc10*

**Non vorremmo esagerare nel valorizzare la figura dell'hacker. Ma è vero che non si è hacker senza amore della conoscenza e desiderio di diffonderla.**

# Password MMC del Nokia 6600: la risposta

*Vorrei rispondere alla richiesta di aiuto da parte di Andrea comparsa a pagina 7 del numero 61. Per risolvere il problema della password della MMC del 6600, si tratta di andare con il programmino FExplorer (o Seleq, è lo stesso) nella cartella Z:\System\ aAps\UnlockMMC. Si esegue poi, cliccandoci sopra, il programmino chiamato unlockMMC.app. Quando richiesto, si inserisce una combinazione di numeri casuali qualsiasi e la MMC dovrebbe risultare sbloccata. Colgo l'occasione per pubblicizzare un sito molto frequentato: http://www.nokiovo.it. Ciauzzzzzzz, Andrea463*

**Grazie a nome di Andrea e tutti quanti avevano bisogno di una dritta sul Nokia 6600.**

# Disco RAM per Linux

*Mi faccio la domanda e mi do una risposta! Vi ho scritto chiedendovi se esisteva un modo per usare la RAM come disco per Linux. Ebbene, l'ho trovato a http://www.linuxfocus.org/English/November1999/article124.html articolo un po' vecchio, ma utile... ciao.*

*Bauz*

**Ciao e grazie per la dritta!**

# Una cascata di googlewhack!

*Due parole italiane che, cercate insieme su Google, danno come risultato un solo sito. Ecco la lista di Luigi, che ha messo al lavoro il suo IRCbot Tavoletta. La lista vera è molto più lunga... abbiamo levato le somiglianze e le volgarità. Anche perché tutti non ci sarebbero mai stati!*
*Grazie Luigi, e se vuoi farci vedere il codice te lo pubblichiamo sicuramente!*

*afide apprensivo*
*ameba autarchica*
*amen satanizzato*
*aracnide retroattivo*
*balalaika assonnata*
*balena capellona*
*cerbiatto impoverito*
*cetaceo zebrato*
*cifosi galoppante*
*contapassi prosciugato*
*cozza idrofoba*
*deflettore introspettivo*
*denominazione nippo-coreana*
*dentifricio nebulizzato*
*destabilizzatore deprimente*
*emorroide insostituibile*
*espediente vermiforme*
*facocero post-moderno*
*formica aracnofobica*
*gabibbo ellittico*
*gambero conquistatrice*
*girarrosto ritorto*
*granseola robotica*
*lanciagranate reggicalze*
*leccalecca paraculo*
*leccapiedi autopulente*
*lineamento acefalo*
*macaco retroattivo*
*marylinmanson cattolico*
*moglianese batterista*
*multipresa mostruosa*
*nettezza macrocefala*
*neurone dispotico*
*ocarina tarchiata*
*oscuratore autoritario*
*palazzine boliviane*
*paracarro forzuto*
*paragnosta perpendicolare*
*parastinchi ridondante*
*pargolo piroettante*
*patentino idrofobo*
*pinolo epilettico*
*piretro cremisi*
*pistillo inesploso*
*poliestere supponente*
*portabiancheria comunista*
*portaombrelli pastoso*
*portapenne cremoso*
*postino poliomelitico*
*prestanome motorizzato*
*protozoo buzzurro*
*ragione effimerica*
*raptus catarifrangente*
*retino roboante*
*rotatoria psichedelica*
*rucola catalitica*
*saltimbanco ripetente*
*scriba ibernato*
*sequoia portalettere*
*sguattera permeabile*
*tartufo positronico*
*termocoperta prussiana*
*tirapiedi monouso*
*torero retrattile*
*trottola sieropositiva*
*truciolo mammone*
*video deframmentabile*
*vinaccia paralitica*
*xilofono maiestatis*

# Driver misterioso

*Mi hanno regalato un masterizzatore SCSI Yamaha modello CRW6416S con controller DC315/U e vorrei installarlo su un pc con Linux Mandrake 9.1.*
*Nel dischetto allegato sono però presenti i soli driver per Windows. Esistono i driver per Linux?*

**Non abbiamo potuto provare personalmente ma ci risulta che l'unità dovrebbe funzionare con l'impostazione mmc3 generica di X-CDRoast (http://www. xcdroast.org/). Prova anche a vedere se ci sono novità su http://people.redhat. com/dledford/.**

*Un oggetto simile sta in un ago e può essere iniettato sottopelle. Da quel momento saremo dei numeri, a radiofrequenza.*

# SIAMO TUTTI

**Tutti noi siamo abituati a passare dalla cassa del supermercato con il carrello pieno.** E a fare la coda aspettando che quello davanti a noi abbia finito. D'ora in poi, basta. I prodotti saranno letti tutti d'un colpo. Niente più cassiera: solo un tornello che si apre con la tessera del bancomat, da cui verrà prelevato il conto. Subito. I nuovi sistemi di identificazione elettronica a onde radio manderanno in pensione senza alcun dubbio tutte le barre possibili.

La nuova tecnologia RFID (Radio Frequency Identification, identificazione a radio frequenza) ha infatti superato ogni immaginazione e forse la troveremo perfino in farmacia: insieme al vaccino antinfluenzale, potremo acquistare il kit per l'identificazione sottopelle. Vediamo come.

## Tutti numerati

**Il chip, della società americana Find Me (www.4verichip.com)**, contiene un codice a 38 bit non alterabile, perché integrato nella scheggia di silicio mentre la incidono. Fatti i conti, sono possibili circa 490 miliardi di numeri unici che identificheranno ogni chip e quindi ogni persona in cui il chip verrà inserito.

La circuiteria necessaria è quasi tutta integrata nel chip stesso, grande quanto un grano di riso, tranne una piccolissima antenna e un micro condensatore per la sintonia. Niente pile, niente alimentazione. Il sistema si alimenta da solo dalle stesse onde radio che riceve e per le quali è stato sintonizzato. Il tutto è inserito in una capsula di vetro lunga 11 millimetri e di 2,1 millimetri di diametro. Le giuste dimensioni per essere infilata in un ago poco più grosso del normale venduto in un kit sterile, con tanto di siringa per l'iniezione sottopelle. La capsula di vetro è biocompatibile ed è perfino spalmata di una sostanza che facilita l'integrazione definitiva con i tessuti del nostro organismo. Dal momento in cui sarà inserita nel nostro corpo saremo perfettamente e univocamente numerati e potremo entrare al supermercato mentre una gentile e automatica voce femminile collegata al data base ci accoglierà

INQUIETANTE

***Nuova frontiera del wireless o grande fratello che si avvera? Un risponditore RFID non lascia scampo. Adesso è perfino iniettabile sottopelle***

**Certo, avvicinarsi al bancomat e prelevare senza nemmeno dire "sono io" può essere una comodità impareggiabile.** Ma può aprire scenari da paura. Chi volesse conoscere di noi ogni spostamento, ogni acquisto, ogni abitudine non avrebbe che da inserirci il chip. Magari subdolamente, durante l'anestesia di un intervento chirurgico, per esempio. O la prima volta che passiamo dal dentista...
Più difficile, ma non impossibile, impossessarsi della nostra identità: identificato il chip con una banale radiografia sarebbe sufficiente una minuscola incisione.
Senza nemmeno arrivare a tanto, se nei nostri calzini sarà inserita un'etichetta RFID avremo già buone probabilità di essere riconosciuti sempre. O spiati sempre.

# IDENTIFICABILI

con una bel "Buona giornata, signor Rossi! Per lei abbiamo riservato alcuni sconti particolari al reparto cosmetici..." Per non parlare del passaggio in autostrada, dell'entrata nel nostro posto di lavoro, dell'ingresso in ospedale o in posta. Se siamo registrati nel database ci sarà consentito l'inverosimile. O saremo vigilati meglio…

## Come proteggersi

**Uno dei problemi che si sta cercando di risolvere è proprio quello del possibile ascolto a distanza.** Il principio su cui si basa RFID è infatti molto semplice: quando il chip è investito da una radiofrequenza opportuna, ne assorbe l'energia per autoalimentarsi e risponde con una emissione radio contenente il flusso di informazioni memorizzate.
Chiunque s'intenda un po' di radioelettronica, con un'antenna direttiva potrebbe mettersi a una distanza tale da non essere visto e rubare le informazioni contenute in uno qualunque di questi chip, aprendo nuovi scenari di spionaggio industriale, militare, sanitario e civile.
Un metodo per evitare l'ascolto a distanza, proposto dall'MIT, il Massachussets Institute of Technology, è quello di cambiare il protocollo di base usato per la trasmissione RFID e adottarne uno chiamato "silent tree-walking". Un sistema proposto da RSA, detto a "pseudonimi", fa emettere all'etichetta RFID identificativi che variano da momento a momento, per cui l'etichetta sembra riferirsi a oggetti diversi secondo il momento in cui la si interroga. Ovviamente chi ha in mano l'elenco degli "pseudonimi" non si lascia ingannare, ma chi non ce l'ha non potrà mai capire a cosa l'etichetta si riferisce. Forse. Intanto Ibm ha investito 250 milioni di dollari in una nuova divisione che si occuperà di RFID e che impiega oltre mille persone. Un segnale nemmeno tanto piccolo di cosa ci accadrà quando andremo al supermercato nei prossimi mesi.

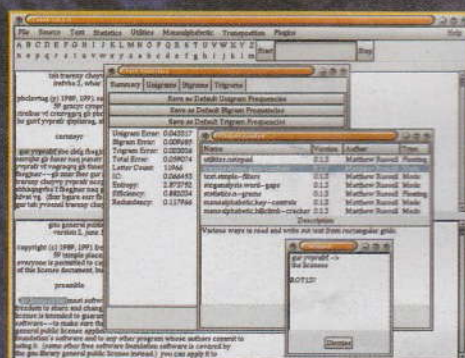
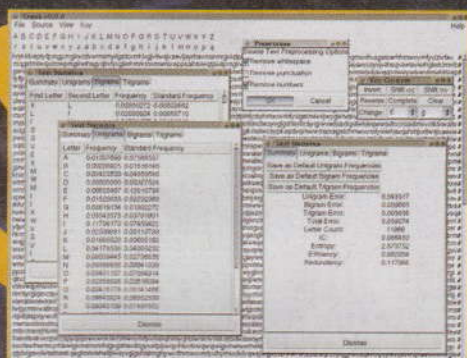
**ControlBus**
**controlbus@softhome.net**

# RSA

***Le security challenge sono la frontiera della crittanalisi. C'è chi ci prova... e rischia di farci i soldi***

**Gli hacker hanno mille interessi. Uno dei più intriganti è il cracking.** C'è cracking buono e cracking cattivo; quello buono consiste nel fare saltare sistemi e codici con l'obiettivo di mostrare che sono deboli, in modo che ne vengano creati di più forti.

**In questo spirito si collocano le sfide lanciate dagli RSA Laboratories:** spostare in avanti la frontiera della crittanalisi, per favorire la creazione di algoritmi più robusti e superiori. Per chi riesce a violare una sfida ci sono premi in denaro di entità non trascurabile. Insomma, ancora una volta chi ha genio potrebbe venire ricompensato adeguatamente!

# CI SFIDA!

*In cerca di strumenti per la crittanalisi? Perché non provare Crank (http://crank.sourceforge.net)?*

## La Factoring Challenge

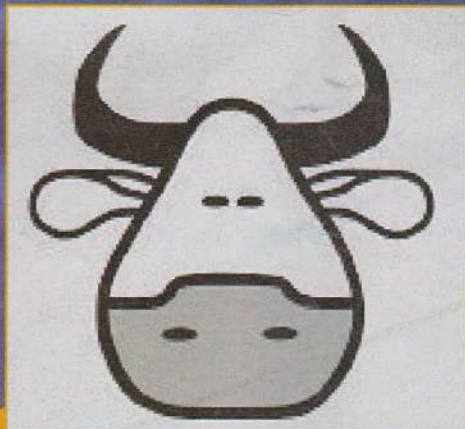
**Numeri molto grandi:** chi riuscirà a fattorizzarli, cioè a scoprire quali numeri primi vanno moltiplicati per ottenerli? I premi variano dai diecimila dollari per la sfida da 576 bit fino ai duecentomila dollari per quella da 2.048 bit. Tutti i particolari si trovano alla pagina http://www.rsasecurity.com/rsalabs/node.asp?id=2092.

## La Secret-Key Challenge

**Una sfida su crittografia DES e dodici basate sul cifrario a blocchi RC5.** Il cifrario DES è a 56 bit e le dodici chiavi vanno da 40 fino a 128 bit. In tutti i casi c'è da indovinare una frase segreta preceduta da tre blocchi di testo, conosciuti, che contengono la frase The unknown message is: (il messaggio sconosciuto è: ). Tutti i particolari si trovano a partire dalla pagina http://www.rsasecurity.com/rsalabs/node.asp?id=2100, compreso il fatto che alcune sfide sono già state risolte. Ne sono ancora vive otto, ognuna con una taglia di diecimila dollari.

**Per aiutare i potenziali solutori sono anche state proposte tredici pseudosfide.** Queste non sono segrete; il messaggio è noto. Non ci sono neanche premi, ma consentono di verificare il funzionamento dei propri programmi… o acquisire pratica sui cifrari RC5.

## La DES Challenge III

**Questa è stata già risolta,** in tempo record, dalla Electronic Frontier Foundation in collaborazione con distributed.net. L'abbiamo citata ugualmente perché è molto interessante anche scoprire che cosa è successo, come è stato craccato il messaggio segreto e altre curiosità. I dettagli stanno sulla pagina http://www.rsasecurity.com/rsalabs/node.asp?id=2108.

## Cracker di tutto il mondo unitevi

**Sono sfide affascinanti, che richiedono impegno e studio e valgono anche soldi.** È praticamente impossibile riuscirci da soli, ma via progetti come distributed.net, per fare un esempio, è possibile formare squadre o entrare in team che hanno probabilità concrete di farcela e aggiudicarsi un premio.
Chi sarà il prossimo a risolvere una sfida? E se fosse un lettore di Hacker Journal? Sarebbe davvero entusiasmante!


**Michele Campovecchio**
**michele_c@hackerjournal.it**


## CHI HA VINTO?

**RSA Security coordina una mailing list dedicata agli annunci delle soluzioni delle sfide.** La lista è a traffico basso e contiene praticamente solo annunci di soluzione oppure informazioni importanti per i partecipanti. Per iscriversi basta inviare a majordomo@majordomo.rsasecurity.com un messaggio contenente nel corpo (non nell'oggetto) la scritta subscribe curious-about-secret-key-challenges. Per disiscriversi è tutto uguale, tranne che la scritta comincia con unsubscribe.

# HACKING

## LINUX LIVE?

**Il termine Linux Live (o meglio Live-CD)** sta ad indicare quelle distribuzioni Linux che possono funzionare direttamente da CD-Rom e che non prevedono installazione. Una distribuzione Live-CD molto famosa è Knoppix.
La distribuzione che stiamo esaminando, Slax, la troviamo qui: http://slax.linux-live.org

## SEQUENZA DI BOOT

**La sequenza di boot rappresenta l'ordine con il quale il BIOS cerca i dispositivi avviabili della nostra macchina.** Un esempio: la sequenza 0 – Floppy, 1 - CD-Rom, 2 - Hard Drive cercherà di bootare prima dal floppy, poi proverà nell'ordine il cd-rom e poi l'hard disk, e si ferma quando trova un device bootabile.
Questa è la configurazione più adatta per eseguire un live-cd.

## E INITRD?

**initrd (cioè Initial Ram Disk) è un file immagine ext2 contenente un filesystem Linux minimale** che serve sostanzialmente per caricare moduli del kernel _prima_ di montare periferiche (per esempio per caricare i moduli per un certo filesystem come reiser).

**La distribuzione che analizziamo è Slax versione 3.0.25.** Vediamo cosa succede al momento del boot in una Linux Live e analizziamo le modalità di caricamento del sistema per andare ad agire nei "punti caldi" della distribuzione.

## Scomporre la ISO

**Per poter analizzare il sistema, dobbiamo innanzitutto possedere un'immagine iso del CD.** Chi ha il C   può farne un dump semplicemente lanciando da una shell Linux, come root, il seguente comando:

```
# dd if=/dev/hdc of=/directory/desiderata/slax.iso
```

**Ovviamente dovremo sostituire /dev/hdc con il vero path del nostro lettore.** Adesso siamo pronti per aprire la iso. Spostiamoci nella directory nella quale abbiamo fatto il dump della iso, creiamo una directory e lanciamo i seguenti comandi sempre da root:

```
# mount -t iso9660 -o loop slax.iso mydir
# cp -rp mydir slax
# umount slax.iso
# rm -rf mydir
# cd slax
```

**Ed ecco che si presentano davanti a noi i file della distribuzione,** che non aspettano altro che essere modificati...

## Al boot

**Se vogliamo eseguire un live-cd dobbiamo entrare nel BIOS e assicurarci che il CD-Rom venga prima dell'hard disk nella sequenza di boot,** altrimenti sarà quest'ultimo ad avviarsi, malgrado la presenza del cd nel lettore. Molto spesso i boot loader come LILO e GRUB sono interattivi e permettono il caricamento di più OS (non è raro trovare una macchina con installati sia Linux, sia Windows e magari anche FreeBS  ), ma nel caso del nostro live-cd no. Il boot loader di slax è isolinux, ed è composto dai file isolinux.bin e isolinux.cfg. Il primo

▲ *Linux Live: ovvero tutto, ma su un solo CD.*

è il boot loader principale (possiamo vedere alcuni possibili messaggi di errore aprendolo con un programma come biew), isolinux.cfg è il file di configurazione. Leggiamolo:

```
# cat isolinux.cfg
display splash
```

**La scomposizione e la modifica di un sistema Linux Live? Niente di più semplice... per un hacker che si rispetti!**

# i un LINUX LIVE-CD

```
default slax
prompt 1
timeout 50

label slax
kernel vmlinuz
append max_loop=255
initrd=initrd.gz init=linuxrc
livecd_subdir=/ load_ramdisk=1
prompt_ramdisk=0
ramdisk_size=7777
root=/dev/ram0 rw lang=it
```

(questo non è l'isolinux.cfg originale ma quello modificato da me. NdX-3mE'89). La prima riga fa visualizzare il file "splash" (possiamo tranquillamente modificarlo con un qualunque editor testuale), la successiva definisce il label di default, quella dopo abilita il prompt "boot:" che permette all'utente di passare parametri aggiuntivi al kernel. "label slax" indica l'etichetta che permette di avviare l'OS del live-cd. L'istruzione "kernel" definisce il file del kernel, al quale verranno passati alcuni parametri: quelli di base sono accanto all'istruzione "append", gli altri vengono passati dall'utente dal prompt "boot:" e sono descritti in "splash". Ma analizziamo quelli di base: a noi interessano soprattutto "initrd=" e "init=". Scomprimiamo e montiamo in loop il file initrd:

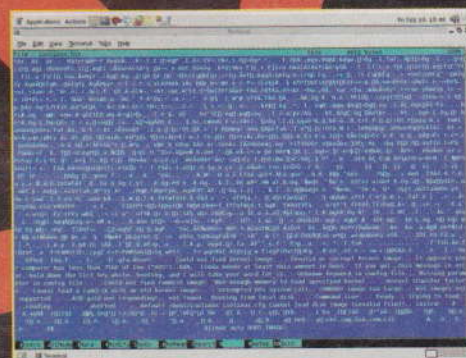
```
# gunzip initrd.gz
# mkdir initrd_mount
# mount -o loop,rw initrd initrd_mount
# cd initrd_mount
```

**Ora possiamo entrare e dare un'occhiata.** A notare il valore del parametro "init=", cioè "linuxrc"; se lanciamo ls nel mount point dell'initrd potremo notare la presenza di un filesystem Linux completo e uno script Bash chiamato linuxrc. Quando lo apriamo vediamo che viene innanzitutto importato un altro file di bourne shell-script (functions) contenente alcune funzioni usate all'interno di linuxrc, poi possiamo arrivare a capire tutte le operazioni svolte da questo file, ovvero: la creazione di un filesystem virtuale, la scompattazione delle immagini, la copia di queste nel filesystem appena creato, il chroot, cioè il cambiamento della directory di root e infine l'avvio del sistema appena spacchettato, al termine del quale ci sarà presentata una schermata d'introduzione e il prompt di login, il che significa che il nostro Linux Live è pronto a obbedire ai nostri comandi.

**IL CONTENUTO DEL FILE LINUXRC**

## Certo, non è finita...

**Finora abbiamo analizzato il boot della distribuzione**, cosa di fondamentale importanza per non commettere errori durante la modifica del live-cd. In un prossimo articolo ci ripromettiamo di analizzare la disposizione del file-system finale all'interno del live cd, come le varie directory (/usr,/bin,/lib,/etc...) vengono montate e i metodi di creazione delle iso. Con le conoscenze appena acquisite possiamo cominciare a divertirci a modificare i parametri in isolinux.cfg e in linuxrc, creare le iso mediante l'utility create_bootiso (possiamo trovarla nella root del filesystem iso principale) e vedere cosa succede. Per provare la iso consigliamo caldamente un emulatore come Bochs, che possiamo trovare su SourceForge.net.
Buon divertimento!

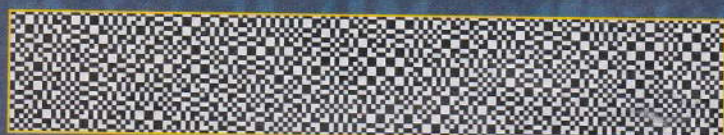
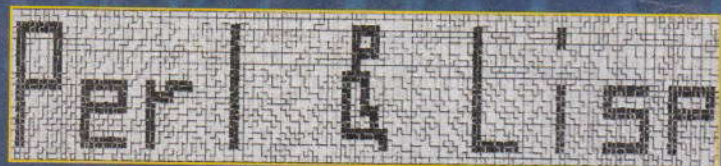
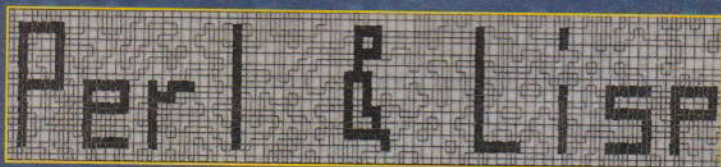
**X-3mE'89**
**http://exxtreme.altervista.org**

▲ *I potenziali errori del bootloader Isolinux.bin.*

# Cifratura VISIVA

001100010101010100010

0001010101000010

***Gemini Nero ci ha mandato una spiegazione del cyberenigma del numero 59 che ci è piaciuta tanto da dedicarle due pagine. Eccola!***

**Questo articolo risolve il cyberenigma e parla un po' di crittografia visiva.** Il primo quesito, quello per tutti, consisteva nel decifrare il messaggio nascosto in due immagini, ognuna delle quali conservava metà del testo originale da indovinare. La soluzione è ovviamente sovrapporre le due immagini in trasparenza:

**Il messaggio nascosto è Perl & Lisp.** La cosa interessante è che esiste più di un modo per mostrarlo:

**La prima schermata è stata ottenuta attraverso una semplice operazione ADD delle due immagini.** La seconda schermata è il risultato della differenza tra le due immagini (ovvero Abs(V1-V2)). La terza immagine è invece il risultato dell'XOR (Exclusive OR) tra le due immagini.

## Il quesito per esperti

**Su questa parte potremmo scrivere un libro... ma saremo più sintetici!** Consideriamo una immagine generica e consideriamo la seguente soluzione:

| Pixel da codificare | Share 1 | | Share 2 | | Sovrapposizione |
|---|---|---|---|---|---|
| bianco | nero/bianco | + | nero/bianco | = | nero/bianco |
| | bianco/nero | + | bianco/nero | = | bianco/nero |
| nero | nero/bianco | + | bianco/nero | = | nero/nero |
| | bianco/nero | + | nero/bianco | = | nero/nero |

**in cui un pixel p viene rappresentato, nella sua versione codificata, da due sottopixel:**

- **se il pixel è bianco,** la coppia di sottopixel usata nella codifica è uguale per le due share, in modo da ottenere, dalla sovrapposizione, una coppia in cui un sottopixel è bianco e l'altro è nero;

• **se il pixel è nero,** la coppia di sottopixel utilizzata in una share è complementare a quella utilizzata nell'altra share, in modo che la sovrapposizione generi una coppia formata da due sottopixel neri.

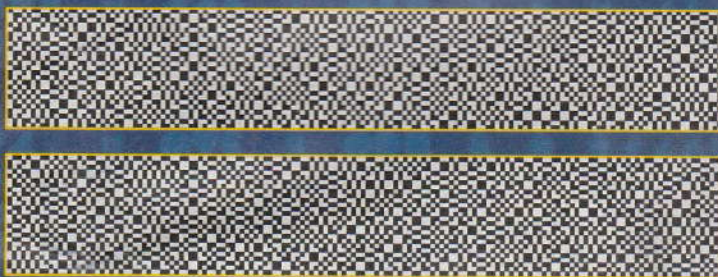
**In pratica un qualsiasi pixel può essere codificato in due modi diversi:** la scelta di quale codifica usare è, per ogni pixel, casuale. Questo sistema di codifica è un caso particolare del più generico schema di crittografia visuale (VCS, Visual Cryptography Scheme) che rappresenta un pixel p con m sottopixel, dove m viene detto espansione del pixel.

**La sicurezza di questo schema è dovuta al fatto che,** osservando una coppia di sottopixel in una share, non è possibile risalire al colore del corrispondente pixel nell'immagine originale. Infatti tale coppia sarà sempre costituita da un sottopixel bianco e un sottopixel nero, indipendentemente dal colore del pixel originale. Si noti come questa rappresentazione dia origine ad un'immagine di larghezza doppia su una dimensione rispetto all'immagine originale. L'immagine risulta deformata, a larghezza doppia e altezza invariata. Ecco un secondo esempio della stessa situazione, con una variazione interessante però.

| Pixel da codificare | Share 1 | | Share 2 | | Sovrapposizione | |
|---|---|---|---|---|---|---|
| | | + | | = | | Quantità di nero = 1/2 |
| | | + | | = | | |
| | | + | | = | | |
| | | + | | = | | |
| | | + | | = | | |
| | | + | | = | | |
| | | + | | = | | Quantità di nero = 1 |
| | | + | | = | | |
| | | + | | = | | |
| | | + | | = | | |
| | | + | | = | | |
| | | + | | = | | |

**Confrontando il primo esempio con questo, si nota una differenza fondamentale.** In questo secondo schema l'immagine codificata dà origine a immagini di dimensione doppia su base e altezza, mantenendo inalterate, questa volta, le proporzioni. Questa soluzione è ottimale quando le immagini sono in biano e nero, mentre per immagini in scala di grigio o a colori esistono altre implementazioni che non differiscono molto da questa (almeno per il caso in scala di grigi).

## Il quesito per geni

**Questo è l'indirizzo del sito che effettua automaticamente la cifratura e che, tra l'altro,** dovrebbe essere quello che è stato usato da Hacker Journal per realizzare il cyberenigma [indovinato! N.d.R]: http://www.leemon.com/crypto/VisualCrypto.html Ecco un altro enigma, per chi avesse particolarmente gradito il gioco:

## Il quesito per super hacker

**Grazie ad una libreria freeware,** il Visual Cryptography Kit ottenibile all'indirizzo http://www.cl.cam.ac.uk/~fms27/, possiamo scrivere un semplice programma di crittografia visuale in Python con pochissime linee di codice:

```
import vck
import sys
import os

def quit(msg=""):
   print "USAGE: python %s
mypicture.tif\n Error:
%s.\n" % (sys.argv[0], msg)
   sys.exit()

try:
   filename = sys.argv[1]
except:
   quit("missing filename")

basename,    ext    =
os.path.splitext(filename)
if ext == "":
   quit("Filename has no
extension")

def doit(root, image=file-
name, base=basename):

   s1, s2, w1, w2 = vck.spli-
tImageG(
      root, filename, base +
"_1.ps", base + "_2.ps")
   wBoth = s1.view(root)

s2.renderOnCanvas(wBoth.
canvas())
   return w1, w2, wBoth

vck.mainApp(doit)
```

**L'esempio è un po' standard,** in quanto la libreria permette dopo una semplice analisi di essere usata con estrema facilità. Il codice si può utilizzare secondo la chiamata

```
python myfile.py mypicture.tif
```

dove myfile.py è il codice in oggetto.

**Gemini Nero**

# A caccia

## Ci siamo mai chiesti cosa succede se un codice a barre viene letto sbagliato? Sopratutto: è un'ipotesi così improbabile?

Altolà! O il codice o la vita.

**Per sbagliare ci vuole proprio poco.** Basta uno scambio di cifre battute velocemente sulla tastiera del nostro pc per crearci dei guai. Pensiamo ai codici della nostra carta di credito, o alle tastiere alle casse di un negozio, o ai codici a barre sporchi che vengono letti male da uno scanner. Di occasioni per commettere errori ce ne sono un'infinità. Per trovare un errore ci vuole un metodo che lo riconosca e, volendo, lo corregga automaticamente.
Un sistema semplice? Riscrivere il codice che stiamo usando un paio di volte. Se uno dei due è diverso dall'altro, c'è stato un errore. Già, ma quale dei due numeri è quello giusto? Boh. Sappiamo che c'è, ma non dove.

**Prendiamo allora il caso del codice a barre usato sui prodotti alimentari.** È fatto di 8 o 13 cifre. Per rapidità guardiamo quello di 8 cifre, tanto il metodo è lo stesso. Come fa il computer attaccato allo scanner della cassa a capire che il codice è stato letto giusto? Usa il carattere di controllo, ovvero l'ultima cifra che appare sul codice a barre. Ecco come.

Anche l'esercito utilizza i codici a barre: speriamo non si sbagli!

### Tutto sommato

**Supponiamo che il nostro codice sia 1234567** (l'ottava cifra è, appunto, quella di controllo che dobbiamo calcolare). Si inizia dalla prima cifra e la si moltiplica per 3. Poi la si somma alla seconda cifra moltiplicata per 1 e si va avanti, prima con 3 e poi con 1, fino a esaurire tutte le sette cifre del codice, così:

$$1 \times 3 + 2 \times 1 + 3 \times 3 + 4 \times 1 + 5 \times 3 + 6 \times 1 + 7 \times 3 = 60$$

**I numeri 3 e 1 sono chiamati "pesi". Ora questo numero lo dividiamo per 10.**

$60/10 = 6$ con il resto di zero.

**Ecco, quello che ci interessa è il resto di questa divisione: zero.**
È il nostro codice di controllo. Quindi il codice a 8 cifre completo è 12345670.

# dell'errore

## Come facciamo a scoprire l'errore?

**Ora facciamo finta che lo scanner del supermercato,** per via di un'etichetta un po' sporca, legga una cifre sbagliata. Il computer riceve, per esempio, il codice 12345870 (il 6 è stato letto come un 8) e ricalcola l'ultima cifra per confrontarla con quella del codice. La cifra sbagliata è in una posizione che ha il peso = 1. Quindi il risultato è:

▲ *Un bel 2,2 % d'errore possibile*

1x3 + 2x1 + 3x3 + 4x1 + 5x3 + 8x1 + 7x3 = 62

63/10 = 6 con il resto di 2

**Il resto è 2.** Prendiamolo con un segno meno davanti e otteniamo -2: ovvero 6 (la cifra giusta) meno 8 (la cifra letta sbagliata). L'errore non verrebbe riconosciuto solamente se calcolando cifra giusta - cifra sbagliata = 0, cosa che accade solo quando la cifra giusta è uguale alla cifra sbagliata. Ovvero quando non c'è errore!

## Non c'è errore!

**E se due cifre vicine sono lette (o battute sulla cassa) invertite?** Vediamo un po'. Il computer riceve, per esempio, il codice 21345670. Le prime due cifre (chiamiamole cifraA e cifraB) sono invertite tra loro. Di quanto cambia la somma? Ecco come calcolarlo: (3 x cifraA + cifraB) – (cifraA + 3 x cifraB) = 2 x (cifraA – cifraB). Ora dividiamo per 10 e guardiamo il resto.

Benissimo, se lo facciamo con le nostre cifre ci accorgiamo che l'errore esiste. Ma ci ricordiamo anche che quando il resto è zero significa che di errori non c'è traccia.

Quando il resto potrebbe essere comunque zero? Se ci pensiamo un attimo, succede tutte le volte che cifraA – cifraB = 5 o viceversa. Per esempio, se la prima cifra 0 ha vicino un 5, o se la cifra 5 ha vicino uno 0, il resto è comunque zero anche se le scambiamo è così sembra che non ci siano stati errori. Questo succede anche quando un 1 viene scambiato con un 6 (o un 6 con un 1), un 2 con un 7 , un 3 con un 8 o un 4 con un 9 (o viceversa). Ovvero in 10 casi non sapremmo dire se c'è o non c'è un errore.

## E quindi?

**Quindi il metodo ha delle probabilità di non funzionare. Quante volte può accadere?**

Cento sono le possibilità di combinarsi di ogni coppia di cifre, per cui 90 sono tutte combinazioni sbagliate che dovrebbero darci un errore, ma dieci di queste 90 non sono rilevabili come errore. Allora la possibilità di beccare l'errore scende a 80/90 = 88,9%.

## Esistono altri metodi?

**Certamente! Il codice di controllo della codifica ISBN dei libri, per esempio, rivela tutto.** La probabilità di beccare l'errore è del 100%. Fantastico. Sarebbe allora possibile usarlo anche per, diciamo, le carte di credito? Si, ma impraticabile. Perché il carattere di controllo può essere anche una X, che sta a indicare un dieci. Immaginiamoci cosa succederebbe quando qualche servizio di vendita telefonica ci chiedesse di battere sulla tastiera del telefono il nostro numero di carta di credito...

Ecco perché nelle carte di credito si utilizza un altro sistema ancora, inventato da Ibm. Che ha il 2,2% di probabilità di fare cilecca. Interessante, ma vedremo il perché un'altra volta…

One4Bus
one4bus@hacker journal.it

▲ *Codice a barre EAN 8: dov'è l'errore?*

ISBN 0-901690-54-6

00725

9 780901 690548

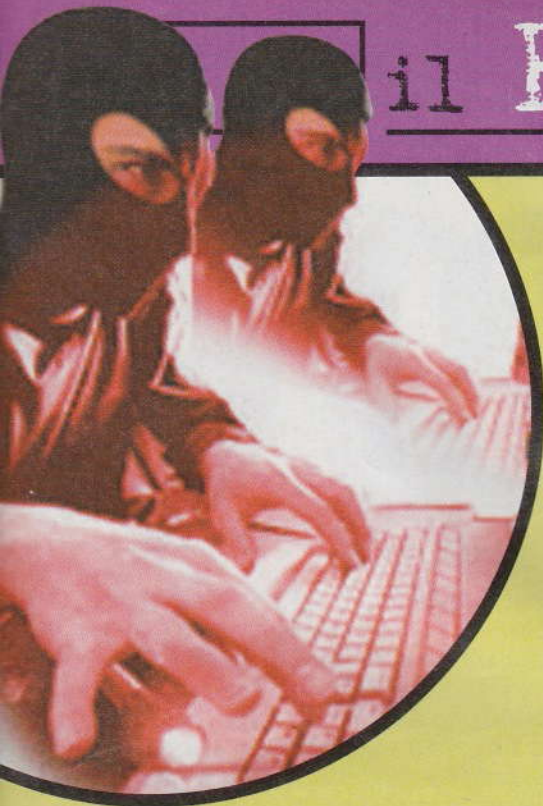
EAN

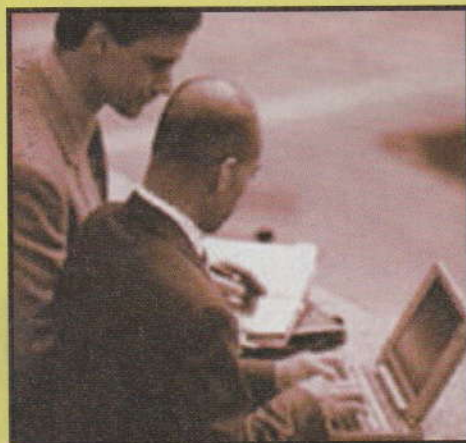
Group

Publisher

Title

Check digit

▲ *Qui l'errore non può esserci*

# Sul FILO del

*"La quantità di decessi, in questo ospedale, è decisamente superiore alla norma!". Stava quasi gridando, ma gli sembravano tutti degli zombie. Erano seduti in una bella stanza illuminata, intorno a un tavolo semicircolare, ampio e spazioso*

**Come capo della security dell'ospedale aveva un bel daffare.** Perché non era solamente incaricato di organizzare al meglio l'attività di qualche buttafuori, quando al pronto soccorso la situazione si scaldava un po' troppo per la presenza delle bande di ragazzotti che accompagnavano l'amico ubriaco, se non accoltellato.

Lo avevano incaricato anche di studiare i report statistici dell'ospedale, a caccia di qualche particolare anomalo. Sempre di sicurezza si trattava, in tempi di informatizzazione spinta.

In un angolo della stanza brillavano dei led arancioni e rossi, che di tanto in tanto sparavano piccoli flash verdi.

## Paranoico?

**La sua preoccupazione era evidente, ma solo a lui.** Dalle ultimi analisi sui dati in suo possesso, che aveva recuperato da un data base del server centrale e trasferito su un foglio elettronico del suo OpenOffice, appariva chiaro che la quantità di persone passate a miglior vita in quel maledetto ospedale era in netto aumento. Anzi, si era fatta preoccupante esattamente da due settimane. Il 13 luglio, giorno del suo compleanno, ebbe il primo sussulto guardando il grafico emerso dai dati. "Fosse stato un picco", stava alzando la voce, "non sarei qui, signori, a dirvi queste cose!".

Il direttore del servizio elaborazione dati lo guardò preoccupato, ma si limitò a dire maliziosamente che non era ancora stato trovato un metodo statistico sufficientemente buono per stabilire che l'aumento dei decessi dovesse veramente nascondere qualcosa di preoccupante. Lo stesso foglio elettronico poteva utilizzare delle funzioni non particolarmente sofisticate, forse a volte imprecise. Poi dipendeva molto dall'esperienza (sì, disse proprio esperienza) dell'utente e da tanti altri fattori che la stessa scienza statistica ammetteva come disturbanti.

C'era poi la questione degli errori dei medici e dell'altro personale. Qui dentro nessuno avrebbe mai ammesso che una quantità di decessi superiore

# WIRELESS

a quella degli incidenti automobilistici era dovuta a scambi di siringhe, lentezze nell'intervento, sbadataggini delle infermiere, quantità invertite nella distribuzione dei medicinali, scorrette diagnosi e malfunzionamenti delle pompe peristaltiche durante le fleboclisi. Eppure era un problema che stava emergendo in tutto il mondo e ogni altra struttura seria, si diceva, ne aveva fatto addirittura oggetto di un apposito ufficio, almeno per salvare la faccia.
Come si poteva pensare che, in questo scenario, un picco di decessi potesse avere una qualche significativa implicazione pratica?

## Nessun allarme

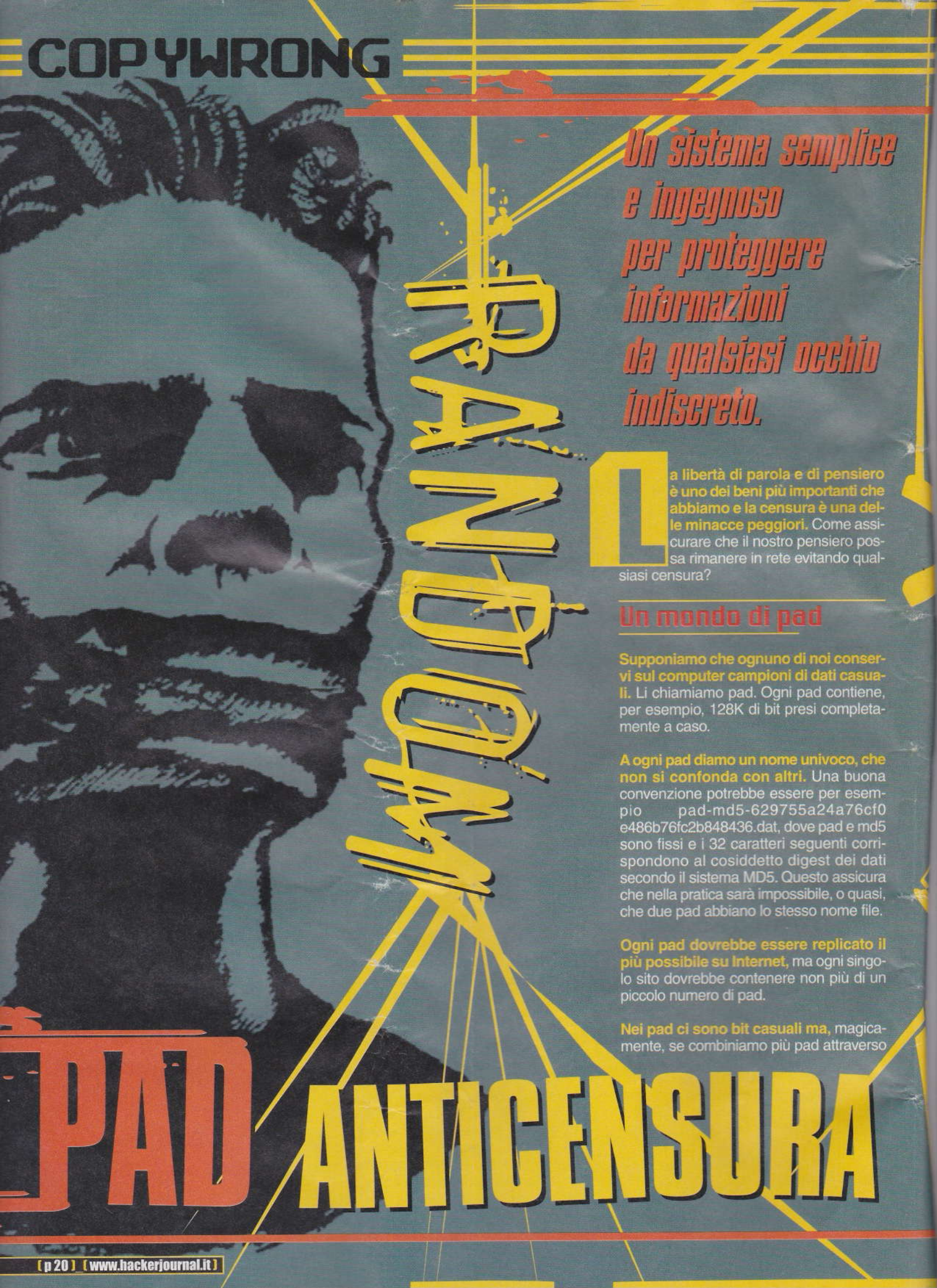
**Erano le dodici e quarantacinque minuti e il direttore si alzò, troneggiando all'altro capo del tavolo.** "Signori, vi ringrazio dell'interessante brainstorming che abbiamo avuto in questa mattinata, splendida mattina direi", disse girando la testa verso l'ampia vetrata. "Mi pare di poter dire che nulla di fortemente preoccupante sia emerso, se non che la nostra attenzione dovrà indubbiamente crescere ancora, rispetto a fenomeni che vedo rientrare nella norma. Buon appetito". Come capo della security, si disse, aveva fatto anche un bel flop, stamattina. Nessuno aveva preso per buone le sue paranoie, o forse lui era uno di quelli ancora convinti che si potessero affermare le cose con la semplice sincerità. Nessuna strategia, nessuna sottolineatura del fatto che la fama di un ospedale fuori norma lo avrebbe portato alla chiusura o almeno alla rimozione di tutta l'alta dirigenza. Non si era sentito di dirglielo. E aveva fatto malissimo. Perché il grafico parlava chiaro.

**Guardando fuori dalla finestra, lo notò seduto su una panchina del bel giardino alberato.** Aveva un notebook sulle ginocchia, appoggiato ai pantaloni di un pigiama azzurrino. Un paziente organizzato, non c'è che dire. Perlomeno ha trovato qualcosa da fare.
Nello spigolo della stanza le lucine dei led erano sempre vive. La sua nuova scheda wireless funzionava che era un piacere. Aveva adottato una Belkin che tirava il segnale dello standard 802.11g dai normali 54 Mbps ai favolosi 125 Mbps. Trasferire i possenti file contenuti nel server centrale era uno scherzo da ragazzi e nella piena libertà di spostamento non rimpiangeva il cavo Ethernet a cui era stato, fino ad allora, costretto. Potenza del WiFi. Si trovò mentalmente a ripercorrere le ultime settimane con il gusto per la tecnologia, che non gli mancava certamente. Da quando su ogni piano occhieggiavano i led colorati dei router wifi, con le loro antennine sporgenti, gli sembrava di essere sempre osservato da piccoli marziani. Ci pensava sorridendo e sempre sorridendo si voltò verso l'ampia finestra. Assaporava la libertà, come quel paziente in pigiama azzurro. Che gli sorrise, a sua volta. Sembrava gli stesse leggendo nel pensiero. Ed era solo un ragazzino. Un ragazzino appassionato, si disse.

## Epilogo

**Poi, fu come un lampo che gli attraversava il cervello.** Corse al suo notebook e attivò la finestra di controllo della connessione. Cercò velocemente la rete wireless a cui era collegato, tra le undici presenti, tante quanti erano i reparti. Un clic sul pulsante funzioni avanzate e un altro su Stato Collegamento. Lesse avidamente, scorrendo l'elenco dei parametri. Numero IP, ok, MAC del dispositivo, ok, velocità, ok, protezione. Oddio, aveva ragione. La protezione: disattivata. Nessuno aveva mai impostato uno straccio di protocollo WEP e tanto meno WPA. Solo uno stupido Disabled.
Stupido, stupido, stupido. Come si stava sentendo lui.
Un clic sul browser e battè velocemente 192.168.0.1. Il gateway di quel piano. Privacy, la password era "privacy". Entrò nel router e lesse l'elenco dei connessi. Un indirizzo si stava scollegando proprio in quel momento. Andò a recuperare con pochi colpi di mouse il file di log e lo fece scorrere al 12 luglio. Ne fece un copia-incolla nel suo excel e creando una base dati l'analizzò. Indirizzo per indirizzo, escludendo quelli che erano sicuramente dei suoi colleghi. Bingo! Ne rimaneva solamente uno. Quello che era anche entrato nel database del server. Lo stesso, il bastardo, che aveva downloadato e uploadato varie volte il lungo elenco dei pazienti entrati e usciti dall'ospedale, sulle loro gambe o su un carro funebre. E si morse il labbro.

**Il ragazzino, nel frattempo, si stava allontanando verso l'uscita, in una bella giornata di sole.**

# PAD ANTICENSURA

*Un sistema semplice e ingegnoso per proteggere informazioni da qualsiasi occhio indiscreto.*

**La libertà di parola e di pensiero è uno dei beni più importanti che abbiamo e la censura è una delle minacce peggiori.** Come assicurare che il nostro pensiero possa rimanere in rete evitando qualsiasi censura?

## Un mondo di pad

**Supponiamo che ognuno di noi conservi sul computer campioni di dati casuali.** Li chiamiamo pad. Ogni pad contiene, per esempio, 128K di bit presi completamente a caso.

**A ogni pad diamo un nome univoco, che non si confonda con altri.** Una buona convenzione potrebbe essere per esempio pad-md5-629755a24a76cf0e486b76fc2b848436.dat, dove pad e md5 sono fissi e i 32 caratteri seguenti corrispondono al cosiddetto digest dei dati secondo il sistema MD5. Questo assicura che nella pratica sarà impossibile, o quasi, che due pad abbiano lo stesso nome file.

**Ogni pad dovrebbe essere replicato il più possibile su Internet,** ma ogni singolo sito dovrebbe contenere non più di un piccolo numero di pad.

**Nei pad ci sono bit casuali ma,** magicamente, se combiniamo più pad attraverso

# LA LISTA DELLA SPESA

**Ciò che serve per partire è tutto qui: Lo script Perl per rimettere insieme i pad:**ftp://quatramaran.ens.fr/pub/madore/PADS/xorpads.pl.
**Altro script Perl utilizzabile:** ftp://quatramaran.ens.fr/pub/madore/PADS/contrib/xorpads2.pl.
**Programma Delphi per Windows che genera pad random e effettua XOR:** XORFiles.zip dalla directory ftp://quatramaran.ens fr/pub/madore/PADS/contrib/ (guardarla tutta!).
**Pad di prova**: al paragrafo Sample Pads della pagina http://www.eleves.ens. fr:8080/home/madore/misc/freespeech.html.
**Pad già pronti:** per esempio http://adware.no/randompads, http://hem.passagen.se/vildman/pads/, http://users.cybercity.dk/%7eccc48268/. C'è una lista più ampia (ma vari link non funzionano) al paragrafo Known Pad Repositories della pagina http://www.eleves.ens.fr:8080/ home/madore/misc/freespeech.html.

*La produzione di numeri casuali è sempre importante per avere informazioni capaci di sfuggire a qualunque censura.*

una funzione XOR otteniamo dati reali, custoditi all'interno dei pad stessi. È importante notare tre cose: primo, nessun pad contiene tutti i dati dell'informazione reale, ma solo una parte di essi; secondo, il proprietario di un pad può non sapere che cosa effettivamente c'è dentro; terzo, in assenza di altre informazioni, il contenuto di un pad è perfettamente indistinguibile da un campione di dati casuali.

## Come fare

**Produrre un pad non è complicato.** Servono 128K di dati random. Servono più pad (almeno tre, meglio cinque, al massimo sette, per la migliore sicurezza ed efficienza) presi in giro per Internet e prodotti da più persone. Prendiamo i dati che vogliamo mettere in sicurezza e ne facciamo un XOR con i pad, usando per esempio Perl. Dai pad che vengono incrociati otteniamo un nuovo pad, composto da nuovi caratteri, sempre casuali. Ma, se facciamo un altro XOR con il pad vecchio, otteniamo il pezzo di file che avevamo nascosto! Il risultato deve essere chiamato con un nome file che abbia le stesse convenzioni degli altri, così che sia impossibile distinguerlo.

## Ricucire i pezzi

**Qualcuno, nella rete che si genera, dovrebbe conservare gli elenchi dei nomi dei pad che, messi insieme, generano un certo file.** Questo qualcuno, possibilmente, dovrebbe conservare pochi pad o nessuno. Per recuperare il file in questione si cerca nella rete l'elenco dei nomi, poi si cercano i pad corrispondenti e si mette insieme il tutto con il programma giusto.

# UNA DOMANDA INSIDIOSA

**Quanto detto è solo teoria; chi sfrutta il sistema dei pad per violare la legge è uno sciocco, come minimo.** Ma si supponga di avere il file di un film, spezzato in più pad. Ogni pad contiene di fatto dati che non sono direttamente quelli del film e ogni computer contiene solo un pezzo di quello che serve per ricostruire il film. Come si può accusare il detentore di un singolo pad di violazione del copyright?

## I pad sicuramente innocenti

**Un pad sicuramente innocente serve a confondere le acque.** I suoi dati sembrano random ma non lo sono, e il contenuto è, appunto, innocente. Qualche esempio:

- **concatenare i digest MD5** di ogni verso della Divina Commedia, di ogni riga della Bibbia o altra opera di pubblico dominio;
- **incrociare in XOR le cifre,** in binario, di pi greco e della radice di 2;
- **prendere una foto di famiglia** e cifrarla con qualsiasi sistema, anche banale.

**Un pad sicuramente innocente serve anche a provare la propria innocenza,** dal momento che è facile mostrare di che cosa si tratta e come è stato generato.

**Se si crea una montagna di pad, molti contenenti dati a caso,** alcuni sicuramente innocenti e altri contenenti informazioni utili mascherate da XOR, queste ultime saranno ragionevolmente al sicuro da ogni tentativo di censura.

**Chi comincia a creare pad?** Se siamo in tanti, ci riusciremo…

**Reed Wright**

# La COMUNITÀ WAREZ e i suoi

**Nel loro complesso, questa specie di club spontanei nati su Internet sono stati chiamati la comunità Warez.** Allora c'era all'incirca una decina di gruppi ben organizzati e molto prolifici, che continuamente alimentavano i lunghi elenchi di software sprotetto recuperabile su siti ad hoc.

## DA DOVE PARTIRE

**Difficile indicare risorse certe;** i siti warez appaiono e scompaiono, tornano dopo lunghi sonni, si reinventano, si travestono... provare a cercare warez in Google, o aggiungere warez all'argomento di qualunque ricerca, è un buon metodo per cominciare un viaggio nei bassifondi di Internet. Un buon sito per approfondire è http://www.davislogic.com/warez.html.

## Uno per tutti: DrinKorDie

**I membri di DrinKorDie erano tecnici, esperti in programmazione, comunicazione su rete e sicurezza.** Oltretutto lo erano anche nella vita normale, presso importanti società di software. Quando le autorità americane iniziarono diverse campagne contro i gruppi organizzati che manipolavano illegalmente il software commerciale, hanno identificato parecchi dirigenti di società rinomate, amministratori tecnici di diverse università statunitensi e non solo, impiegati d'alto livello, studenti e perfino impiegati in uffici governativi. Alcuni membri di Drin-

*All'inizio degli anni '90 diversi gruppi che si stavano affacciando a Internet si sono organizzati per sproteggere software commerciale, poi distribuito gratuitamente sulla rete.* ***Erano nati gli Warez!***

# SEGRETI

KorDie erano gli stessi sviluppatori di software che firmavano le pre-release e le immettevano contemporaneamente a disposizione dei gruppi warez.
Il gruppo è stato forzatamente sciolto da una famosa operazione condotta dall'F-BI, che recuperò una quantità impressionante di hardware zeppo di file illegali, già nel 2001.

## Chi glielo fa fare?

**DrinKorDie e gli altri gruppi warez modificano il software e lo sproteggono generalmente per i semplice gusto di farlo.** Il "crack" di un pacchetto software è un'azione che richiede delle conoscenze non banali, una gran voglia di sperimentare nuovi metodi, spesso fantasia e certamente gusto della sfida. Inoltre permette di vivere una certa sindrome di Robin Hood, che ruba ai presunti ricchi per ridistribuire ai poveri.
Difficilmente per ottenere software da un sito warez è necessaria una qualche iscrizione e, se lo è, di norma è completamente gratuita.

## Una delle ultime operazioni

**Fastlink è stata una delle ultime retate di siti, e non solamente di quelli,** effettuate dal Dipartimento della Giustizia americano nel 2004, ai danni di una notevole quantità di gruppi considerati illegali. Oggi la più combattuta è la pirateria musicale, ma generalmente i siti warez non sono particolarmente specializzati. Anzi, spesso non sono per nulla siti. Spesso, molto spesso, i veri canali di circolazione di software illegale, o di tutto l'altro materiale coperto da copyright, sono i canali IRC e le reti peer-to-peer, dove avviene lo scambio diretto di file dopo aver dato un'occhiata al "catalogo" di ciascun computer collegato.
Oggi, sotto le pressioni delle case discografiche, la persecuzione ai siti e ai canali di scambio di materiale warez continua a un ritmo sempre più serrato. Come già abbiamo avuto modo di registrare in altre occasioni, si è arrivati a perseguire anche duemila singole persone per scambio illegale di file MP3.
Per non parlare delle pasticciate leggi di cui ogni stato, non solo l'Italia, si sta dotando. Salvo poi non tenere conto delle infinite possibilità di Internet e quindi cadere addirittura nel ridicolo pensando di poter facilmente bloccare i flussi di dati tra utente e utente.

**Nyarlathotep**
**nyarlathotep@hackerjournal.it**

## ALL'OMBRA DELLA BSA

**In Italia gli exploit contro i gruppi e le iniziative warez erano prerogativa della polizia postale.** Sempre più spesso oggi, invece, a muoversi è la Guardia di Finanza, pilotata dalla branca italiana della BSA (Business Software Alliance). Da noi comunque ci sono poche iniziative di vero hacking alternativo, onesto o disonesto, e molta più bassa pirateria d'accatto che fa girare per la Rete videogiochi e altro materiale di grande consumo. Il primo grande colpo contro la comunità warez in Italia fu in ogni caso l'Italian Crackdown di dieci anni fa, che colpì oltre duecento BBS. Si andava ancora con i modem a 1,2 Kbps… sull'Italian Crackdown è stato scritto un ottimo libro, che si può leggere in edizione integrale su http://www.apogeonline.com/openpress/libri/529/.

# Un'IDEA per CIFRARE

**IDEA è un cifrario a blocchi descritto per la prima volta nel 1991 da Xuejia Lai e James L. Massey della Eidgenössische Technische Hochschule (ETH) di Zurigo.** Consiste in una revisione minore di un cifrario preesistente, il Proposed Encryption Standard o PES; il suo nome originale infatti fu IPES, o Improved PES. IDEA è stato usato nelle prime versioni di PGP.

**L'idea di IDEA nasce nell'ambito di un contratto di ricerca siglato dall'ETH con la Fondazione Hasler e si concretizza anche in un brevetto posseduto dalla svizzera Ascom, il numero 5.214.703 per gli Stati Uniti.**
Ma il suo uso non commerciale è assolutamente libero. Inoltre il brevetto scadrà, tra il 2010 e il 2011 secondo la nazione interessata.

## Come funziona

**La chiave di IDEA è a 128 bit,** mentre l'algoritmo opera su blocchi di 64 bit, in otto trasformazioni che vengono dette round e una trasformazione finale dell'output chiamata half-round.

## SICUREZZA QUASI A POSTO

**IDEA è a tutt'oggi un algoritmo privo di gravi falle di sicurezza.** Sono state individuate alcune classi di chiavi più deboli di altre, ma sono così rare che non è neanche necessario escluderle esplicitamente.
A tutt'oggi nessun attacco è riuscito a superare più di cinque degli otto round e mezzo previsti dall'algoritmo.

## OPERAZIONE XOR

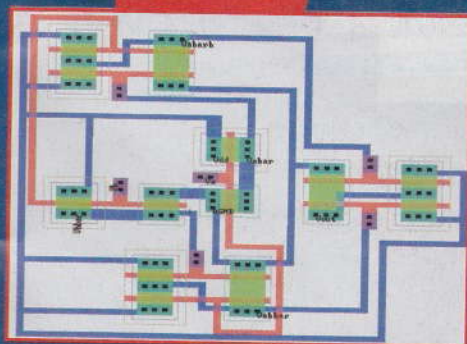
| PRIMO BIT IN INPUT | SECONDO BIT IN INPUT | BIT DI OUTPUT |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Nonostante l'età e i progressi di hardware e software, IDEA resta ancora oggi un buonissimo algoritmo di cifratura.

*L'operazione logica XOR confronta due bit in input e dà come risultato un bit in output. Un bit di input proviene dal testo da cifrare e un bit proviene dalla chiave. L'uno e l'altra sono suddivisi in sottoblocchi da sedici bit.*

## SE LO DICE BRUCE

**Bruce Schneier, progettista di Blowfish,** ha scritto nel 1996 Secondo me [IDEA] è l'algoritmo a blocchi migliore e più sicuro pubblicamente disponibile in questo momento. Nel 1999 ha fatto parzialmente marcia indietro per via dei progressi registrati nella crittanalisi e della disponibilità di algoritmi più veloci, per non parlare del fatto che i brevetti non sono simpatici a nessuno. Ma IDEA rimane tuttora una buona scelta di sicurezza.

# Guardiamo dentro il cofano dell'International Data Encryption Algorithm per la cifratura supersicura

▲ *XOR, o OR esclusivo. Una funzione molto potente!*

**Il segreto della sicurezza di IDEA sta nella mescolanza di addizioni,** moltiplicazioni e operazioni logiche XOR. Le addizioni sono modulo 2^16 e le moltiplicazioni sono modulo 2^16+1. Le word di valore zero (32 bit tutti a zero) sono considerate come 2^16. Ogni blocco di input, da 64 bit, viene diviso in quattro sottoblocchi da 16 bit. La chiave è di 128 bit e viene preventivamente trasformata in una pseudochiave da 832 bit.
Da questi vengono presi i sottoblocchi K1, K2, K3, K4, K5 e K6. Seguendo le frecce si può capire come vengono incrociati e manipolati i vari sottoblocchi.
Ogni simbolo corrisponde a una delle tre operazioni possibili: addizione, moltiplicazione oppure XOR. Lo schema viene ripetuto otto volte.

**L'operazione XOR confronta bit per bit i due operandi e restituisce un bit zero o un bit uno,** in funzione della coppia di bit in entrata, come si vede nella tabella.

**P. Greco**
**p.greco@hackerjournal.it**

# SPACCHIAMO la LUCE

**Ecco come fare uno strumento semplicissimo e veramente da super-hacker:** il suo nome scientifico è spettroscopio. Noi lo realizziamo con una scatola di corn flakes e un Compact Disk registrato.
A cosa serve? Per riprodurre l'arcobaleno. A che scopo? Qui sta il bello.
Con un po' di pazienza è possibile capire, dall'arcobaleno che ne viene fuori, da

*Per scoprire quale materiale sta bruciando basta guardare il colore della fiamma*

## COME COSTRUIRLO

**Sfruttiamo il fatto che un CD registrato ha la superficie suddivisa in una specie di finissimo reticolo,** dovuto ai 'pit' – i piccoli incavi della registrazione – , e che quindi è una superficie perfetta per realizzare quel fenomeno fisico che è la diffrazione della luce.
Quando un raggio di luce concentrato va a sbattere contro il CD, le diverse frequenze che compongono la radiazione si riflettono con angolature differenti. Per il nostro occhio frequenze differenti significano colori differenti: così vediamo l'arcobaleno.

**La luce è hackerabile? Ebbene sì! Possiamo capire com'è fatta spaccandola in mille pezzi tramite un CD zeppo di dati e una semplice scatola di corn flakes!**

# in TANTI PEZZI!

*► L'occhio umano può vedere le onde eletrromagnetiche la cui lungezza d'onda è compresa tra i 400 e i 700 milionesimi di millimetro. Sotto ci sono gli infrarossi e sopra gli ultravioletti.*

che materiale è generata una certa luce. Che poi è quello che fanno gli astrofisici per capire, dalla luce emessa dalle stelle, di che cosa queste sono formate.
O è quello che serve ai chimici, per sapere cosa c'è dentro una sostanza che colora una fiamma. Si guarda l'arcobaleno generato dalla fiamma e si sa cosa sta bruciando. Interessante. Ancora di più se lo possiamo fare con un CD usato e una scatola di cereali vuota.

StandardBus
standardbus@softhome.net

**Fig.1_Prendiamo una scatola di cereali vuota, chiudiamola bene con dello scotch e poi con le forbici,** o un taglierino, facciamole un taglio a 45 gradi in cui infiliamo un CD, come in figura. Sulla scatola, in corrispondenza della superficie del CD che è rimasta dentro la scatola, facciamo un buco di circa due centimetri di lato.

**Fig.2_Ecco come si presenta il buco sopra il CD.** Notiamo che abbiamo sigillato con dello scotch nero (va bene qualunque cosa) i lati della fessura in cui abbiamo infilato il CD. Il tutto deve essere a tenuta di luce, tranne che per i buchi appositamente fatti.

**Fig.3_In corrispondenza al lato opposto al CD,** facciamo una fessura sottile. Per avere una visione migliore dell'arcobaleno, è bene che tale fessura sia precisa nel taglio. Ci conviene quindi fare un buco rettangolare e poi coprirlo con un cartoncino di qualità migliore, in cui abbiamo fatto la fessura, lunga circa due centimetri e mezzo, o giù di lì.

**Fig.4_Ora puntiamo la fessura sottile,** davanti alla scatola, contro una sorgente luminosa. Per esempio una lampadina. Tenendo la scatola verso la luce e guardando dentro il buco fatto sopra il CD, spostando un po' la testa individueremo un punto in cui si vede una piccola striscia con l'arcobaleno, riflessa dal CD dentro la scatola. Ecco messo a fuoco l'interno della scatola, proprio sulla superficie del CD. L'arcobaleno è ben visibile e vediamo il tipico spettro di una luce bianca: dal rosso scuro al violetto passando per l'arancio, il giallo, il verde, l'indaco e il blu.

FIG.1

# IL CD E L OCCHIO

**La radiazione che l'occhio può vedere è un insieme di onde elettromagnetiche la cui lunghezza d'onda è compresa tra i 400 e i 700 milionesimi di millimetro.** Le piccole buchette che si formano su un CD registrato hanno una dimensione paragonabile e quindi la superficie di un CD è perfetta per scomporre la radiazione luminosa nelle sue diverse lunghezze d'onda. Poi ci pensa il nostro occhio a capire che una lunghezza d'onda maggiore tende al rosso e una minore al violetto.

Il nostro occhio, tra le altre caratteristiche, è anche più sensibile alle lunghezze d'onda al centro dello spettro, che quindi ci appaiono sempre più luminose di quelle agli estremi. Per quanto ci sforziamo, quindi, nel nostro spettroscopio non vedremo mai i colori con la stessa intensità tra il centro e i bordi. Anche se provassimo a puntare una luce più forte.

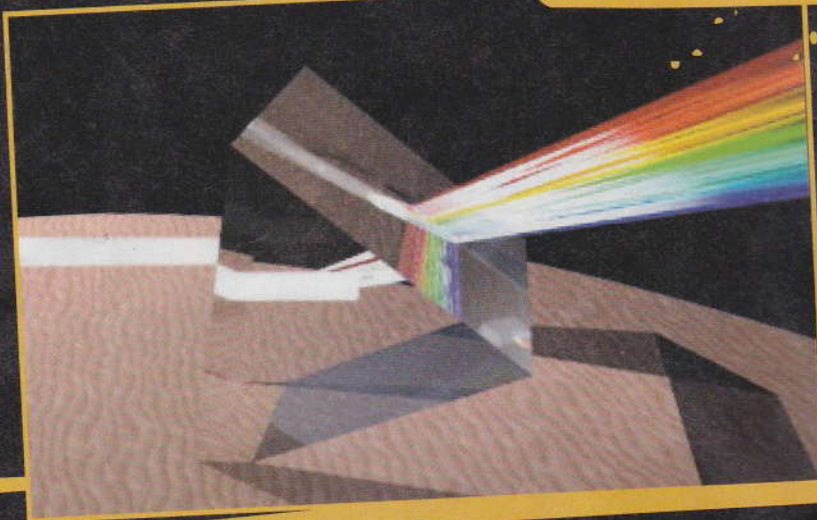



**Fig.5_Ora possiamo usare il nostro strumento e divertirci ad analizzare lo spettro di diverse sorgenti luminose.** Qui la luce bianca naturale, del sole. La stampa sulla rivista cancella un po' di sfumature e soprattutto i toni più freddi, come il violetto. Ma se guardiamo bene con il nostro strumento, dopo il blu vediamo una colorazione viola molto scura e sempre più sfumata. Dopo il violetto si entra nell'ultravioletto, ma il nostro occhio non è in grado di percepirlo.

**Fig.6_Puntiamo il nostro sofisticato strumento portatile contro la luce di un tubo al neon.**
Lo spettro c'è ancora praticamente tutto, ma notiamo una caratteristica strana e differente da prima: alcune zone di colore sono più intense, mentre altre sono più attenuate.
Vediamo quindi delle linee più luminose di altre.
Che cos'è successo? La lampada al neon in realtà contiene diverse sostanze e tra queste il mercurio. Le linee più luminose sono dovute al fatto che il mercurio emette uno spettro tutto suo.

**Fig.7_Lo spettro tipico del mercurio:** questo lo abbiamo scaricato da un sito internet dedicato alla spettroscopia. Se lo confrontiamo con l'arcobaleno della luce al neon vediamo che c'è proprio coincidenza: le linee che vediamo più luminose corrispondono alle linee dello spettro del mercurio.

FIG.4

FIG.5

FIG.6

**Fig.8_Tutto diverso se puntiamo il nostro generatore di arcobaleni contro una lampadina a risparmio di energia.**
Come nella lampada al neon è presente mercurio, ma anche altre sostanze e le linee più luminose si moltiplicano. E' comunque evidente la differenza con lo spettro uniforme e completo della bianca luce solare.

**Fig.9_Abbiamo provato a guardare una lampada a ultravioletti,** di quelle che si usano in discoteca per rendere fluorescenti le camicie bianche... Ovviamente lo spettro s'è ridotto a sole tonalità di blu, tendenti al violetto. L'ultravioletto non possiamo vederlo per via dell'insensibilità del nostro occhio.
Ora non c'è che divertirsi a puntare e guardare. La luce di una candela, di un led, di una fiamma al buio...
Chi riesce a fotografare e a inviarci qualche esempio di arcobaleno?

FIG.7

FIG.8

FIG.9

# ENCICLOPEDIA dell'Hacking!

## Directory Climbing

"Chiamata anche Directory Trasversal o Backticking, è la tecnica che consente di spostarsi all'interno delle directory del computer sotto esame, sfruttando un semplice trucco di notazione dei percorsi, ancora consentito in molti casi e derivante dal vecchio ambiente Unix e DOS (Disk Operating System). È spesso sufficiente anteporre a qualunque nome di file si voglia raggiungere sul computer una serie di coppie di punti, eventualmente separate da uno slash, per esempio: "../../..". Questo indica al computer obiettivo di risalire nell'albero delle directory di tante directory precedenti quante sono le coppie

### ESEMPIO

**Proviamo a collegarci a un sito qualunque**, tramite l'URL: http://www.coffeeuniverse.com/.
Otteniamo la pagina home del sito.

Ora scegliamo un'altra pagina, con un clic su un link , per esempio Coffee Quiz.

L'URL varia, com'è giusto, in
http://www.coffeeuniverse.com/quiz.html

Proviamo ora ad aggiungere in fondo a questo indirizzo lo slash seguito dai due punti /..
ottenendo quindi

http://www.coffeeuniverse.com/quiz.html/..
e premiamo return.

Torniamo come d'incanto alla home, anche se l'URL non corrisponde a quanto avevamo scritto all'inizio. Perché i due punti hanno costretto il sistema a saltare di directory.

### Requisiti

È sufficiente avere un browser e un po' di fantasia. Anche se un server nel suo complesso è stato protetto da questo tipo di intrusioni è facile provare la tecnica rimanendo all'interno delle pagine del sito stesso.

### Security

È sempre necessario, da parte di chi imposta l'organizzazione del sito, fare in modo di controllare quanto è scritto dall'utente che vi accede, sotto forma di URL. Ad ogni URL deve corrispondere una pagina, altrimenti va rifiutata.Sicuramente è necessario evitare che con questa notazione si possa retrocedere nell'albero saltando la pagina home e andando sulla root del computer server.

**LINK:** Qui si spiegano dei metodi sotto Unix di spostarsi velocemente tra directory: http://www.trilug.org/~chilcote/Unix/tree-climbing.html

# ENCICLOPEDIA dell'Hacking!

## Telnet

"TELNET È UN PROTOCOLLO DI RETE CHE CONSENTE DI INVIARE COMANDI A UN SERVER REMOTO. È UTILIZZATO PER PILOTARE DA REMOTO SISTEMI UNIX E APPARATI DI RETE, COME SWITCH E ROUTER. NOI NORMALMENTE CHIAMIAMO TELNET SIA IL PROTOCOLLO, OVVERO L'INSIEME DI REGOLE PER MANDARE COMANDI IN REMOTO, SIA IL PROGRAMMA CHE CI CONSENTE DI COLLEGARCI AL SERVER E INVIARGLI I COMANDI. QUANDO USIAMO TELNET, APRIAMO IN REALTÀ UNA CONNESSIONE TCP SU UNA QUALUNQUE PORTA DEL COMPUTER REMOTO E QUINDI LE INVIAMO I COMANDI SOTTO FORMA DI TESTO.

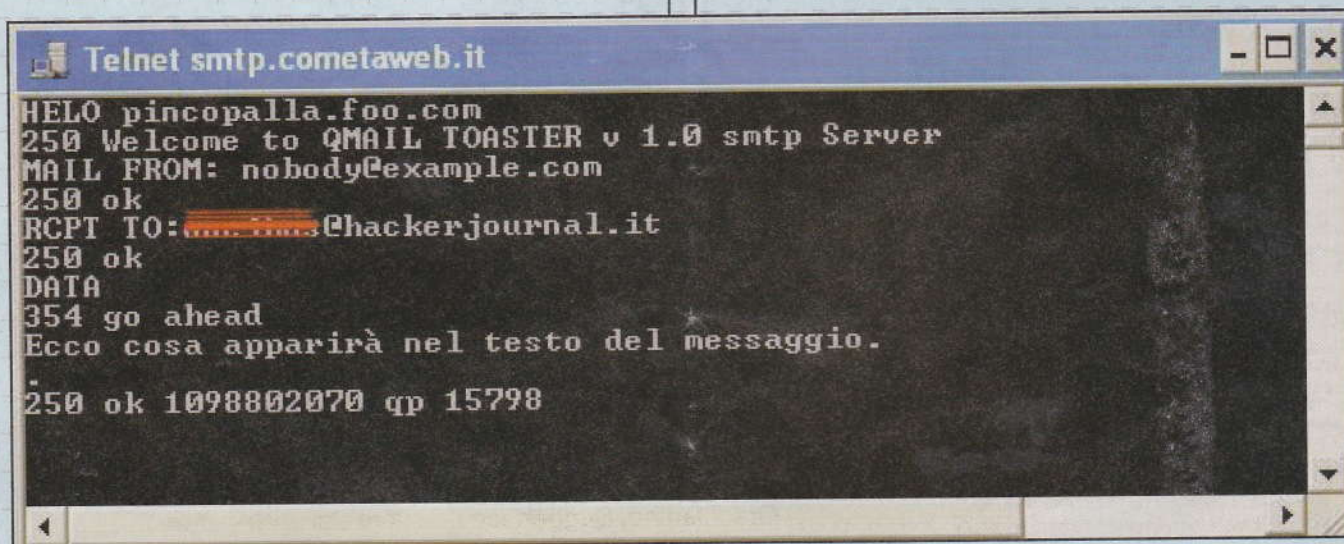
### ESEMPIO

**Ci colleghiamo a un server** di posta in uscita, smtp, alla porta 25:

o smtp.serveresempio.it 25

A connessione avvenuta (non con tutti i server di posta è possibile, dipende dalle protezioni che hanno adottato), scriviamo

**HELO** pincopalla.foo.com
**MAIL FROM**: nobody@example.com
**RCPT TO**: redazione@hackerjournal.it
**DATA**
Ecco il testo che apparirà nel messaggio.

Abbiamo così inviato un'email direttamente da un server smtp, anche se non è quello su cui siamo autorizzati.

### Requisiti

**Possiamo fare delle prove con Telnet aprendolo direttamente in Windows:**
Start > Esegui > telnet
Scrivendo Help otteniamo tutti i comandi e i parametri che possiamo dare al prompt di telnet.

### Security

Attenzione all'uso che si fa di Telnet. Un uso di telnet su un server SMTP come quello descritto può far cadere facilmente nel reato di spamming: è infatti possibile inviare email da server su cui non si possiede un account. Ovviamente se questi non sono sufficientemente protetti.

**UN ALTRO SERVIZIO TELNET CURIOSO**:
telnet towel.blinkenlights.nl
Una patch Microsoft e la descrizione di come difendersi dal mail relay con Microsoft Exchange Server, 2000 e XP:
http://support.microsoft.com/default.aspx?scid=kb;en-us;q304897

**PER SAPERNE DI PIÙ:**
www.yuki-onna.co.uk/email/smtp.html

# POSTA SPLIT: LE RISPOSTE!

HJ59: AVEVAMO PROPOSTO UN MESSAGGIO SEGRETO CON CIFRATURA... VISIVA. LE DOMANDE ERANO LE SEGUENTI

*Paloo ha passato la copertina allo scanner e poi ha assemblato il messaggio con Paint Shop Pro 7*

## Le domande

**PER TUTTI:** Riesci a leggere il messaggio?

**ESPERTI:** Riesci a pensare a un altro metodo visuale di cifratura per mandare messaggi senza che il destinatario debba conoscere una chiave?

**GENI:** Riesci a trovare un sito Web che effettua automaticamente la cifratura?

**SUPER HACKER:** Riesci a scrivere un programma che cifra visualmente un messaggio dato, possibilmente dietro inserimento di una passphrase di cifratura?

mascherina forata che, sovrapposta al primo foglio, mostra solo il messaggio. Ci sono naturalmente numerosi altri sistemi. Chi ne trova altri?

**GENI:** Il sito http://www.leemon.com/crypto/VisualCrypto.html, per esempio, effettua automaticamente la cifratura visiva da noi usata.

**SUPER HACKER:** I programmi sono stati numerosi. Bravi!

*La soluzione di NOU*

## Chi ha risposto

**PER TUTTI:** Paloo; JimB0Th, jimb0th@cappellin.net; M@rk01; Giacomo; -@andromeda@ ; to... [illegible]

*Fatto a mano! Da _.-< PrimematuM >-._*

**GENI:** il PRIMO ARRIVATO è Dirk: anticamente si "cifrava" invertendo il codice con uno specchio (come faceva Leonardo da Vinci) e a http://stereo.jpn.org/eng/ c'è una raccolta completa di software Java per stereogrammi; Alby86av1, stereografia e il programma StereoCreator (quello a http://www.eyetricks.com/stereograms/onlinetools/stereocreator.htm?) ; Lux, http://www.dia.unisa.it/~ads/corsosecurity/www/CORSO-9900/vcs/; TDK e Biondo, http://www-lce.eng.cam.ac.uk/~fms27/vck/; AlexLooJuam, http://marcio.altervista.org/alfabeto_farfallino.php; Jg53Garand, una marea di siti (tra cui http://www.cs.fsu.edu/~yasinsac/group/slides/burke2.pdf; Leroj, il suo sito è a http://leroj.altervista.org/;

*By LukeSnake e dark88*